



PATENT
B422-240 (25813.247)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Shinichi Yamazaki, et al.
Serial No. : 10/640,607
For : COMMUNICATION SYSTEM AND MANAGEMENT
APPARATUS AND METHOD FOR RESTRICTING FUNCTIONS IN
COMMUNICATION SYSTEM
Filed : August 13, 2003
Examiner : Beemnet W. Dada
Art Unit : 2135

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

CLAIM TO BENEFIT OF 35 U.S.C. § 119
AND FILING OF PRIORITY DOCUMENTS

Claim is made herein to the benefit of 35 U.S.C. § 119 of the filing dates of the following
Japanese Patent Application Nos.: 2002-247899 (filed August 28, 2002) and 2003-189924 (filed
July 2, 2003), certified copies of which are filed herewith.

Dated: February 23, 2007

COWAN, LIEBOWITZ & LATMAN, P.C.
1133 Avenue of the Americas
New York, New York 10036-6799
Tel. (212) 790-9200

Respectfully submitted,

John J. Torrente
John J. Torrente
Reg. No. 26,359
An Attorney of Record

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to:
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

John J. Torrente

Signature

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年 8月28日
Date of Application:

出願番号 特願2002-247899
Application Number:

[ST. 10/C]: [JP 2002-247899]

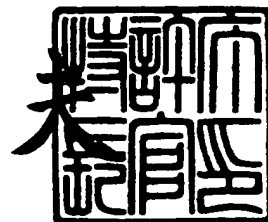
出願人 キヤノン株式会社
Applicant(s):

CERTIFIED COPY OF
PRIORITY DOCUMENT

2003年 9月16日

特許庁長官
Commissioner,
Japan Patent Office

今井康



BEST AVAILABLE COPY

出証番号 出証特2003-3075588

【書類名】 特許願

【整理番号】 4675040

【提出日】 平成14年 8月28日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 1/00

【発明の名称】 会議システムの管理サーバ

【請求項の数】 10

【発明者】

 【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社
社内

 【氏名】 山▲崎▼ 信一

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

【代理人】

 【識別番号】 100087446

 【弁理士】

 【氏名又は名称】 川久保 新一

【手数料の表示】

 【予納台帳番号】 009634

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9704186

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 会議システムの管理サーバ

【特許請求の範囲】

【請求項 1】 ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、

認証手続きを行う際に用いる認証情報に基づいて、参加者の立場を判別する参加者判別手段を有することを特徴とする会議システムの管理サーバ。

【請求項 2】 請求項 1 において、

上記複数の電子機器は、電子機器との間で情報を送受信する会議システムの管理サーバと、近距離無線通信方式で接続することを特徴とする会議システムの管理サーバ。

【請求項 3】 請求項 1 または請求項 2 において、

上記参加者判別手段は、主催者と参加者とを判別する手段であり、

上記会議システムの管理サーバは、操作制限を行う操作制限テーブルを有するサーバであることを特徴とする会議システムの管理サーバ。

【請求項 4】 請求項 3 において、

上記操作制限テーブルで制限される項目として、上記参加者判別手段が判別した主催者と参加者について、広域ネットワークへの接続制限の項目を含むことを特徴とする会議システムの管理サーバ。

【請求項 5】 請求項 4 において、

接続された端末機器について、IPアドレスを割り当てると同時に、IPアドレステーブルを作成するIPアドレステーブル作成部を有することを特徴とする会議システムの管理サーバ。

【請求項 6】 請求項 5 において、

上記IPアドレステーブル作成部で作成されたIPアドレステーブルと、ネッ

トワークに接続されたゲートウェイが持つ I P アドレステーブルとを、共有し、記憶する I P アドレス記憶部を有することを特徴とする会議システムの管理サーバ。

【請求項 7】 請求項 1 ～請求項 6 のいずれか 1 項において、

上記近距離無線通信は、B l u e t o o t h であることを特徴とする会議システムの管理サーバ。

【請求項 8】 ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、

認証手続きを行う際に用いる認証情報に基づいて、上記認証手続きを行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする会議システムの管理サーバ。

【請求項 9】 ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムにおいて、

認証手続きを行う際に用いる認証情報に基づいて、上記認証手続きを行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする会議システム。

【請求項 1 0】 請求項 1 ～請求項 9 のいずれか 1 項において、

上記認証情報は、B l u e t o o t h における P I N コードであることを特徴とする会議システムの管理サーバ。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、会議システムに係り、特に、会議システムの参加者の立場の判断、および会議システムにおける機能制限の割り当に関する。

【0002】

【従来の技術】

従来の会議では、紙ベースで発表資料を参加者全員に配布しているので、資源が無駄であるという問題があり、また、資料が人数分揃わない場合には、不足部数を慌ててコピーし、会議の進行を妨げるという問題がある。

【0003】

ところで、近年は、発表者が、PCやPDAを、会議室に持ち込み、プロジェクタで投影し、プレゼンテーションするのが一般である。さらに、発表者以外の参加者にも、紙ベースではなく、ネットワーク経由で、資料データを配布することによって、上記問題が解決されている。

【0004】

しかし、参加者が多い会議で、全員がネットワークを使用すると、配線が複雑になるという新たな問題が生じる。そこで、Bluetooth等の無線通信を用いた会議システムが考えられている。

【0005】

Bluetooth方式は、アドホックなマルチポイント接続を行うので、最大接続数が、8機器、通信範囲が10mのピコネットを構築し、通信することができ、通信速度に関しては、非同期通信において、下り721Kbps、上り57.6Kbpsの通信が行える。また、音声通信もサポートし、1つのチャンネルで、音声とデータとを転送することができる等、多種多様なプラットフォームでの利用が期待されている。

【0006】

上記Bluetooth等の無線通信を用いた会議システムによって、配線の煩雑さは解消されるが、無線接続による外部からの不正アクセス、データの改ざん等セキュリティ面で、別の問題が浮上している。しかも、一度認証を通過してしまうと、資料のコピー、プリントアウト、データの上書き等の制限は、Bluetoothの認証レベルでは実行することができない。

【0007】

これに対して、特開 2 0 0 1 - 3 1 2 4 7 2 公報では、異なる 2 種類の P I N コードを用いて認証することによって、セキュリティレベルを向上する方法が提案されている。また、特開 2 0 0 1 - 3 3 1 4 3 1 公報では、会議中の権限を、各端末に指定し、機能を制限することが提案されている。

【 0 0 0 8 】

【発明が解決しようとする課題】

特開 2 0 0 1 - 3 3 1 4 3 1 公報では、参加者の機器に権限を与える際に、会議システムのアプリケーション上から、各参加者がタブを選択し、権限を設定する方法をとっている。

【 0 0 0 9 】

しかし、このようにすると、参加者の手間がかかる上、任意に権限の設定を変更することができ、権限を故意に変えてデータを操作することも可能であるという問題がある。

【 0 0 1 0 】

本発明は、会議システムのデータの不正な改ざんや情報の漏洩を防ぎ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことを目的とするものである。

【 0 0 1 1 】

【課題を解決するための手段】

本発明は、ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、認証手続きを行う際に用いる認証情報に基づいて、参加者の立場を判別する参加者判別手段を有することを特徴とする会議システムの管理サーバを提供する。

【 0 0 1 2 】

また、本発明は、ネットワークを介して、会議に参加するユーザによって操作

される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、認証手続きを行う際に用いる認証情報に基づいて、上記認証手続きを行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする会議システムの管理サーバを提供する。

【0013】

また、本発明は、ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムにおいて、認証手続きを行う際に用いる認証情報に基づいて、上記認証手続きを行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする会議システムを提供する。

【0014】

【発明の実施の形態および実施例】

〔第1実施例〕

図1は、本発明の第1実施例である無線通信装置WC1を示すブロック図である。

【0015】

無線通信装置WC1は、会議システム管理サーバ101と、アクセスポイント102と、ゲートウェイ103と、PCまたはPDA104とを有する。

【0016】

PCまたはPDA104は、主催者や参加者が持参したBluetoothによる無線接続が可能なPCまたはPDAである。

【0017】

会議システム管理サーバ101は、広域ネットワークへアクセスするために必要であり、会議システムのアプリケーションを動作させるサーバである。

【0018】

アクセスポイント102は、無線端末から根幹のLANに接続する際に必要と

なるポイントである。また、アクセスポイントは、根幹の LAN に接続され、一般的なスイッチングハブのような役目をする。持参した PC や PDA を有線で会議サーバに接続する場合、ハブを用いて会議システム管理サーバ 101 に複数台接続することができるが、無線接続する場合は、各機器をアクセスポイントに接続し、会議システム管理サーバ 101 との間で、データをやりとりする。

【0019】

アクセスポイント 102 へ接続する場合、セキュリティを考慮し、ユーザ認証の手続きを行う必要がある。一般的に、PINコード (Personal Identification Number) を交換することによって、ユーザ認証するが、アクセスポイントのデフォルト PINコードが固定であると、一度接続したことのある人なら、何度でも接続でき、セキュリティ面で問題がある。

【0020】

そこで、会議の主催者が、予めデフォルト PINコードで、アクセスポイント 102 に接続し、会議の時にのみ有効な PINコードに変更する方法が採られている。

【0021】

しかし、デフォルト PINコードが固定であると、誰でも設定を変更できるので、デフォルト PINコードを故意に変更することもできる。すると、正規の主催者が、会議の時にのみ有効な PINコードに変更しようと考え、固有のデフォルト PINコードで接続しても、接続できないという事態が生じる。

【0022】

そこで、会議室予約システム等で会議室を予約した時に、その会議室付属のアクセスポイント 102 のデフォルト PINコードが設定され、同時に、主催者にメール等で通知し、主催者は、会議予約システム 101 から通知された PINコードを使ってアクセスポイント 102 に接続し、会議の時にのみ有効な PINコードに変更する手段がとられている。参加者は、主催者から予め通知された会議の時にのみ有効な PINコードを含む参加証を持って、会議室に臨み接続する。

【0023】

図 2 は、上記実施例における会議システム管理サーバ 201 を示すブロック図

である。

【0024】

会議システム管理サーバ201は、主制御部202と、ネットワーク通信部203と、記憶部204と、入力部206と、表示部207と、テーブル作成部208と、判別部209と、データベース205とを有する。

【0025】

ネットワーク通信部203は、主制御部202の指示に従い、有線通信網、無線通信網に接続される各種無線端末104との間で、データを送受信する。

【0026】

主制御部202は、会議システム制御、各種アプリケーションの管理、入力部、表示部を制御し、記憶部204は、テーブル作成部208で作成された各種テーブルデータやファイル管理を行う。

【0027】

入力部206は、キーボード、マウス等によって入力を制御し、表示部207は、CRTモニタ等の表示を制御する。テーブル作成部208は、IPアドレステーブルや機能制限テーブル等各種テーブルを作成する。判別部209は、ネットワーク通信部203によって取得した参加証から、会議の主催者であるか、参加者であるかを判別する。

【0028】

図3は、上記実施例において、会議の主催者が会議に参加するまでの動作を示すフローチャートである。

【0029】

まず、会議の主催者は、会議室予約システム等で会議室の予約を行い（S301）、会議の時にのみ有効なPINコードに、設定を変更し（S302）、PINコードを、会議の参加者に電子メール等で通知する（S303）。

【0030】

次に、メールアドレス、PINコード、社員ID等が記されている参加証ファイルを作成し（S304）、この作成したファイルを、参加者全員にそれぞれ配布し（S305）、会議に参加する（S306）。

【 0 0 3 1 】

図 4 は、上記実施例において、会議の参加者が会議に参加するまでの動作を示すフローチャートである。

【 0 0 3 2 】

まず、主催者が配布した会議の時にのみ有効な P I N コードを、参加者が取得する（S 4 0 1）。このときに、電子メールのみでなく、主催者が作成した W e b 等にアクセスして、主催者が配布した会議の時にのみ有効な P I N コードを取得するようにしてもよい。

【 0 0 3 3 】

次に、主催者が配布した参加証を、参加者が受け取り（S 4 0 2）、参加者はその参加証を持参して、会議に参加する（S 4 0 3）。この場合においても、参加証に、P I N コードが記載されているので、会議の時にのみ有効な P I N コードを取得する処理（S 4 0 1）を省くようにしてもよい。

【 0 0 3 4 】

図 5 は、上記実施例において、主催者がアクセスポイント 1 0 2 の P I N コードを変更する処理を示すシーケンス図である。

【 0 0 3 5 】

まず、アクセスポイント 1 0 2 のデフォルト P I N コードを、L A N に接続された P C 等から設定する（S 5 0 1）。この P C には、会議室予約システムが運用され、会議室予約システムは、会議室を予約した際に、自動的に P I N コードが作成され、アクセスポイント 1 0 2 のデフォルト P I N コードに設定し、同時に、予約者に通知するような機能を有する。

【 0 0 3 6 】

次に、主催者は、アクセスポイント 1 0 2 に、接続要求を発行する（S 5 0 2）。アクセスポイント 1 0 2 は、接続要求を受け、データが正しければ、接続確立のメッセージを無線機器に送信し、接続が確立する（S 5 0 3）。

【 0 0 3 7 】

その後に、アクセスポイント 1 0 2 が認証要求を発行し、パスワードの要求を促す（S 5 0 4）。主催者側の端末は、会議室予約システム等で新たに設定され

たデフォルト P I Nコードを送信し（S 5 0 5）、P I Nコードが正しければ、アクセスポイントから認証完了が通知される（S 5 0 6）。

【0 0 3 8】

次に、主催者側の端末が、P I Nコードの設定変更要求を発行し（S 5 0 7）、アクセスポイント 1 0 2 から、要求メッセージ受信応答が帰ってきたら（S 5 0 8）、会議の時にのみ有効な P I Nコードを送信する（S 5 0 9）。アクセスポイント 1 0 2 は、新たな P I Nコードを受信し、P I Nコードの設定を変更し、変更完了のメッセージを主催者に送信し、接続処理が完了する（S 5 1 0）。

【0 0 3 9】

図 6 は、上記実施例において、参加者が会議に参加する場合の処理を示すシーケンス図である。

【0 0 4 0】

参加者は、アクセスポイントに、接続要求を発行し（S 6 0 1）、アクセスポイント 1 0 2 は、接続要求を受け、データが正しければ、接続確立のメッセージを無線機器に送信し、接続が確立する（S 6 0 2）。

【0 0 4 1】

その後、アクセスポイントが認証要求を発行し、パスワードの要求を促す。参加者の端末は、会議の時にのみ有効な P I Nコードを送信し（S 6 0 4）、アクセスポイント 1 0 2 から認証完了のメッセージを受信したら（S 6 0 5）、予め配布された参加証を、アクセスポイント 1 0 2 を経由して、会議システムに送信する（S 6 0 6）。会議システムは、参加証を受信したら、受信応答を参加者の端末に送信し、接続処理が完了する（S 6 0 7）。

【0 0 4 2】

図 7 は、上記実施例において、会議システム管理サーバの判別部 2 0 9 における動作を示すフローチャートである。

【0 0 4 3】

参加証には、最低限 P I Nコードが記述されていることを前提とし、参加証に記述されている P I Nコードが 2 種類（デフォルト P I Nコード、会議の時にのみ有効な P I Nコード）あり（S 7 0 1）、しかも、会議システム管理サーバ 1

01が保持しているPINコードと一致すれば(S703)、接続相手を主催者と判別し、主催者としての機能権限を与える(S706)。

【0044】

一方、PINコードが1種類(会議の時にのみ有効なPINコード)であり(S701)、しかも、会議システム管理サーバ101が保持しているPINコードと一致すれば(S702)、参加者であると判別し、参加者としての機能権限を与える(S704)。不正なPINコードが記述された参加証を受信すれば、不正なアクセスとみなし、全ての操作を不能にする(S705)。

【0045】

図8は、会議システムによって制限される機能のテーブルを示す図である。

【0046】

[第2実施例]

上記会議システム管理サーバ101では、参加者それぞれにIPアドレスを割り当て、広域ネットワークへアクセスすることができるシステムが考えられる。しかし、この場合、参加者がWebのメールサービス等で重要な情報を故意に外部に漏らす可能性が考えられる。

【0047】

本発明の第2実施例は、上記会議システム管理サーバ101が受信した参加証に、最低限PINコードが記述されていることを前提に、参加証に記述されているPINコードによって、広域ネットワークへのアクセス制限をかける実施例である。

【0048】

具体的には、上記会議システム管理サーバ101へ接続したときに取得する参加証に記載されているPINコードが、2種類(デフォルトPINコード、会議の時にのみ有効なPINコード)であり、しかも、会議システムが記憶し、保持しているデフォルトPINコード、会議の時にのみ有効なPINコードと一致すれば、主催者であると判別し、広域ネットワークへ接続できるIPアドレスを割り当てる。

【0049】

P I Nコードが、1種類（会議の時にのみ有効なP I Nコード）であり、しかも、正しいP I Nコードであれば、参加者であると判別し、広域ネットワークへ接続できないI Pアドレスを割り当てる。会議システム管理サーバ101のI Pアドレス取得方法は、L A Nに接続されているゲートウェイ103が持つI Pアドレステーブルを取得し、共有することで行う。

【0050】

具体的には、無線端末104が会議システム管理サーバ101に接続したときに、会議システム管理サーバ101は、ゲートウェイ103が持つI Pアドレステーブルを取得する。これと同時に、会議管理サーバが取得する参加証に記載されているP I Nコードに基づいて、主催者であるか、参加者であるかを判別し、広域ネットワークへのアクセスを許可できる無線端末に対してI Pアドレスを配布する。

【0051】

今回は、ゲートウェイが持つI Pアドレステーブルの取得を、無線端末の接続と同時にを行ったが、一定時間間隔テーブルを取得するようにしてもよい。

【0052】

また、取得したI Pアドレステーブルに、そのI Pアドレスを追加し、ゲートウェイに送信することによって、ゲートウェイ103と会議システム管理サーバ101とで、I Pアドレステーブルを共有する。

【0053】

第2実施例によれば、主催者と参加者とで広域ネットワークへのアクセス制限をかけることによって、不正な外部アクセスを防ぐことができる。

【0054】

以上のように上記実施例によれば、予め電子メール等で配布される会議参加証に記載されているP I Nコードを用いて会議の参加者か主催者かを判別し、データのアクセス制限をかけることでデータの不正な改ざんを防ぐと共に制限の設定をアプリケーション上で別個に行う手間を省くことができるという効果を奏する。

【 0 0 5 5 】**【発明の効果】**

以上のように本発明によれば、会議システムのデータの不正な改ざんや情報の漏洩を防ぎ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことができる。

【図面の簡単な説明】**【図 1】**

本発明の第 1 実施例である無線通信装置 W C 1 を示すブロック図である。

【図 2】

上記実施例における会議システム管理サーバ 2 0 1 を示すブロック図である。

【図 3】

上記実施例において、会議の主催者が会議に参加するまでの動作を示すフローチャートである。

【図 4】

上記実施例において、会議の参加者が会議に参加するまでの動作を示すフローチャートである。

【図 5】

上記実施例において、主催者がアクセスポイント 1 0 2 の P I N コードを変更する処理を示すシーケンス図である。

【図 6】

上記実施例において、参加者が会議に参加する場合の処理を示すシーケンス図である。

【図 7】

上記実施例において、会議システム管理サーバの判別部 2 0 9 における動作を示すフローチャートである。

【図 8】

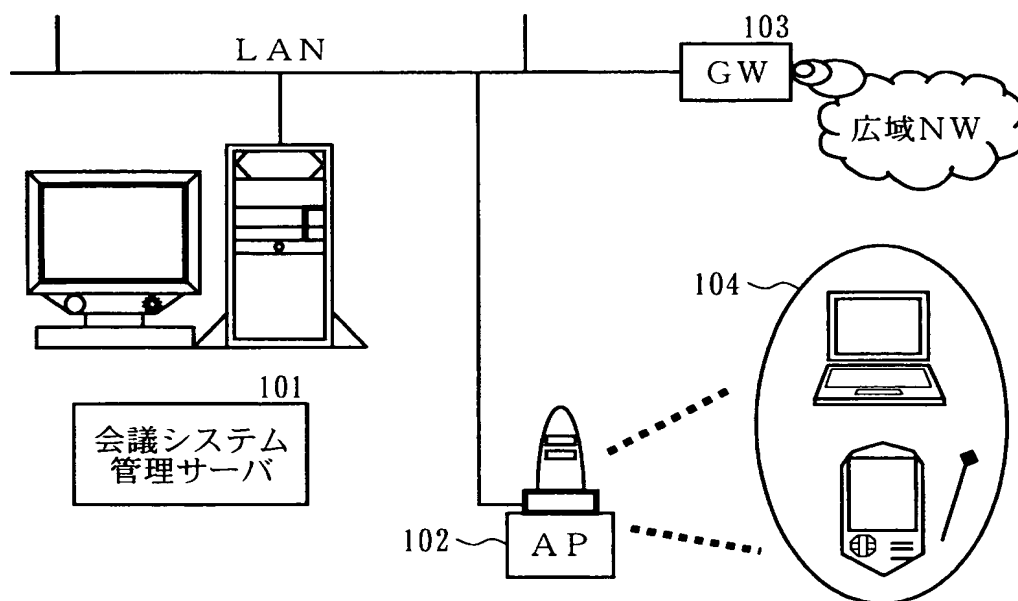
会議システムによって制限される機能のテーブルを示す図である。

【符号の説明】

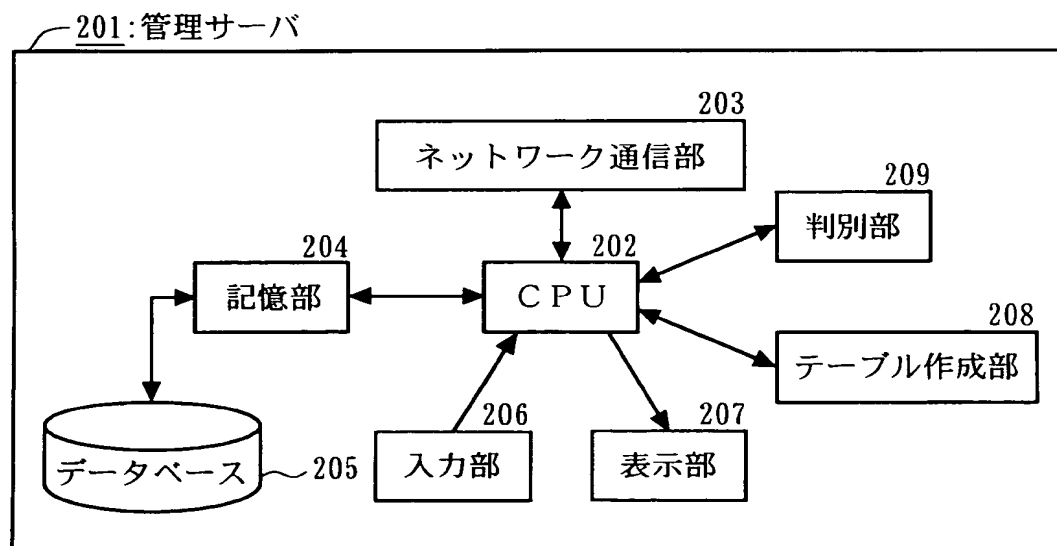
WC 1 …無線通信装置、
1 0 1 …会議システム管理サーバ、
1 0 2 …アクセスポイント、
2 0 1 …管理サーバ、
2 0 3 …ネットワーク通信部、
2 0 4 …記憶部、
2 0 5 …データベース、
2 0 8 …テーブル作成部、
2 0 9 …判別部。

【書類名】 図面

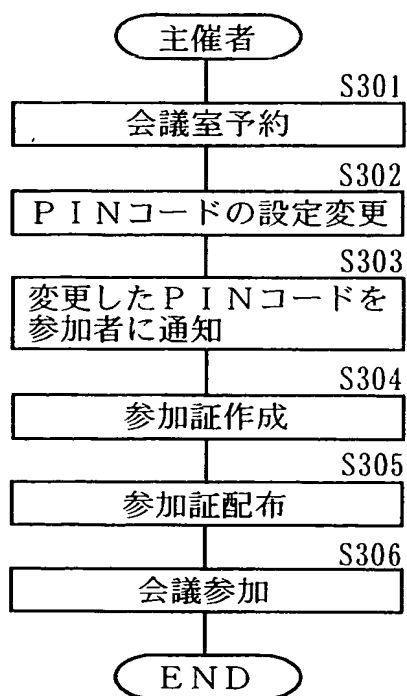
【図 1】

WC 1 : 無線通信装置

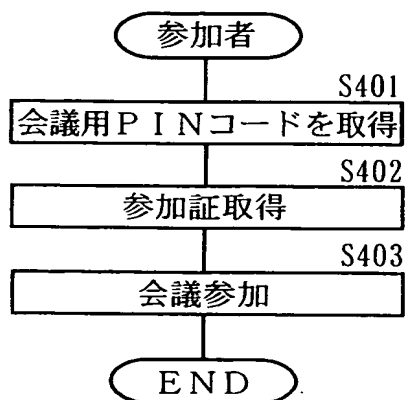
【図 2】



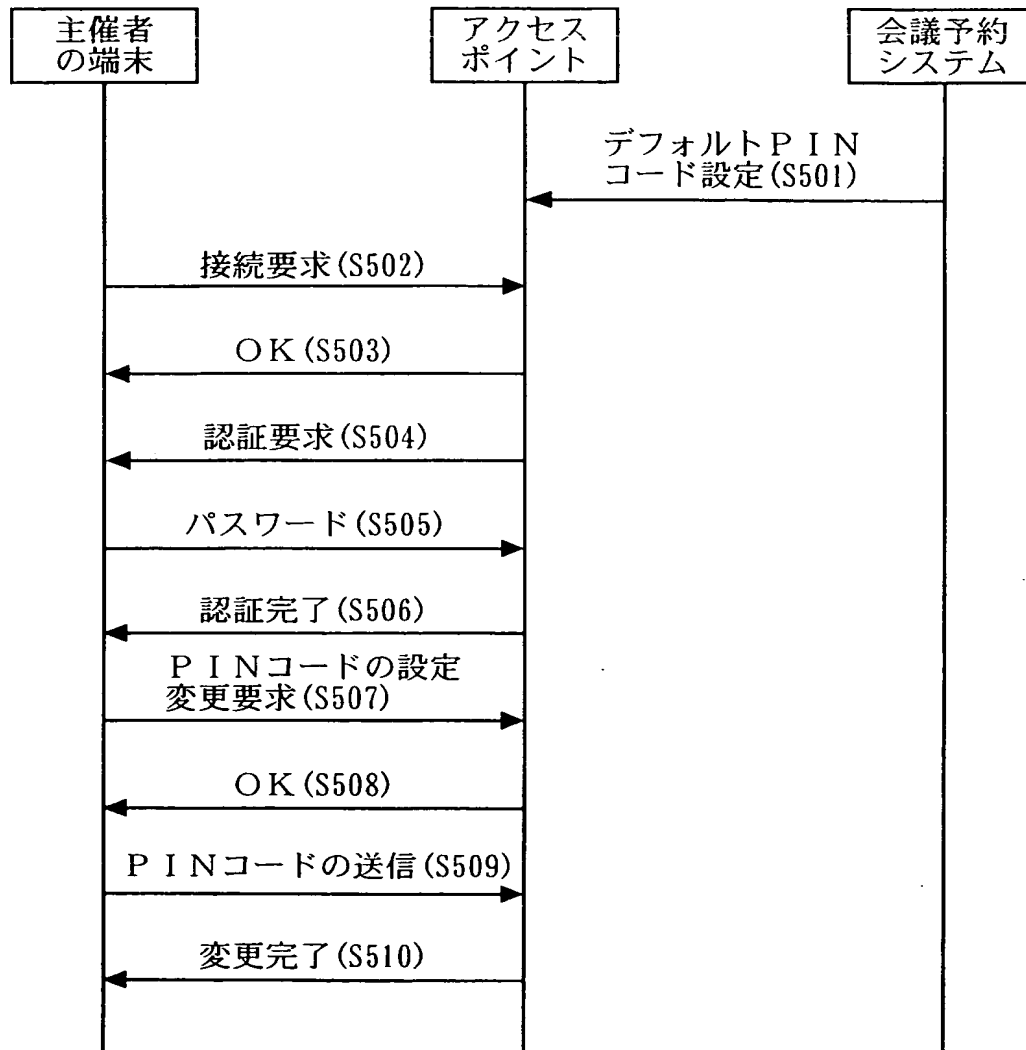
【図 3】



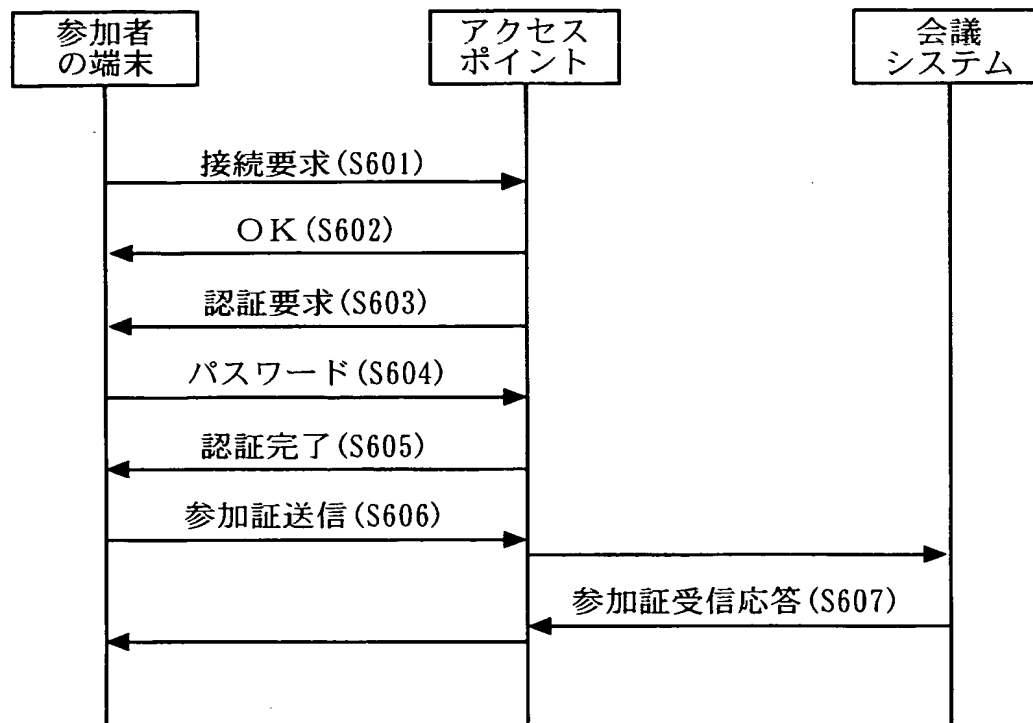
【図 4】



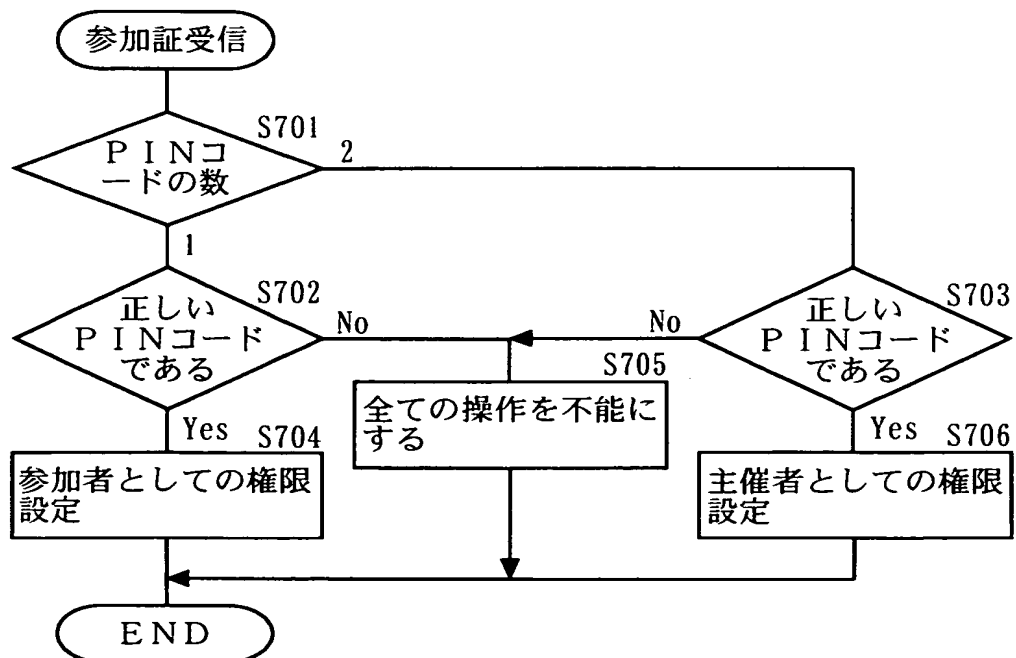
【図 5】



【図 6】



【図 7】



【図 8】

機能	主催者	参加者
ファイルの閲覧	○	○
ファイルコピー	○	×
ファイル削除	○	×
ファイル印刷	○	×
ファイル名変更	○	×
ファイル上書き	○	×
ファイル保存	○	×
ネット閲覧	○	△
I P アドレスの変更	○	×
P I N コードの変更	○	×
メール送受信	○	×

【書類名】 要約書

【要約】

【課題】 会議システムのデータの不正な改ざんや情報の漏洩を防ぎ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことができる会議システムの管理サーバを提供することを目的とするものである。

【解決手段】 ネットワークを介して、会議に参加するユーザによって操作される複数の電子機器と、電子機器との間で、情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される会議システムの管理サーバにおいて、認証手続きを行う際に用いる認証情報に基づいて、参加者の立場を判別する参加者判別手段を有することを特徴とする会議システムの管理サーバである。

【選択図】 図 1

特願 2 0 0 2 - 2 4 7 8 9 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 1 0 0 7]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キャノン株式会社